UNITED STATES DISTRICT COURT
FOR THE
DISTRICT OF VERMONT

UNITED STATES OF AMERICA,	)	
	)	
v.	)	Case No. 2:21-cr-66
	)	
SCOTT REMICK,	)	
Defendant.	)	

DEFENDANT'S MOTION TO SUPPRESS EVIDENCE

AND

REQUEST FOR A *FRANKS* HEARING

Now comes Scott Remick and submits this motion to suppress evidence.[1] The initial warrants issued in this case lacked probable cause and included material omissions or false statements. Later warrants were not independent but were sought only as a result of tips obtained because of publicity surrounding and must be suppressed as fruit of the poisonous tree. This case is unique in that all parties agree that it originated after a hacker invaded a computer alleged to belong to Mr. Remick and then contacted law enforcement.

Procedural Background

Following a tip by a hacker (the "SOI"), the government sought a warrant to remotely access computers using Mr. Remick's internet provider to connect to the internet. *See* Doc. 5 (the "Remote Access Warrant"). At the same time, the government sought a warrant to search Mr. Remick's home and electronic devices.

[1] To the extent necessary, the defendant seeks leave to exceed the applicable page limit set forth in Local Civil Rule 7(a)(4), made applicable by Local Criminal Rule 1(b).

See Doc. 1 (the "Hardscrabble Road Warrant"). After remotely accessing a computer on July 3, 2021, the government executed the Hardscrabble Road warrant on July 7, 2021, and arrested Mr. Remick. He was charged by complaint with possession of child pornography and released on conditions. Mr. Remick was charged in a July 22, 2021 indictment with possession of child pornography.

Some months later, the government sought several additional warrants related to its belief that Mr. Remick had obtained child pornography from a 17-year-old minor approximately 10 years ago. See Docs. 34 (Megc7 warrant), 43 (Facebook warrant), 53 (Seized Devices warrant). Mr. Remick was charged in a June 2, 2022 nine-count superseding indictment, which charged him with possessing child pornography, distributing child pornography, receiving child pornography (3 counts), and producing child pornography. The Court has declared the case complex. Mr. Remick remains on pretrial release.

Factual Background & Probable Cause

The remote-access warrant application presented to the Magistrate Judge offered that on June 16, 2021, a source of information both called and emailed the Vermont State Police to report its belief that someone in Bristol, Vermont, possessed child pornography. The warrant application indicates that the SOI came across the alleged child pornography by hacking a computer alleged to belong to Mr. Remick. The application reproduced the hacker's email to the Vermont State Police, which included a photo of Mr. Remick's driver's license, the IP address the hacker claimed to have observed, and a text file listing directory and file names. The warrant application indicated that the text file was not thought to contain a

complete listing of the files. Doc. 5-3 at 7. The application claims that while the text file lists file names only, the filenames "indicated that the files likely contained child exploitation material." Doc. 5-3 at 7.

The application indicates that agents spoke with the SOI on June 17, 2021, and that the SOI stated that:

> He/she is a private software developer and security analyst. The SOI is part of a small group of individuals involved in analyzing a very specific piece of software with a specific security vulnerability. As part of this work, this group has developed a software "bot" to search for computers/servers using this specific piece of software, which still have this known security issue. The bot identified a computer (part of the Target Media) with this security flaw (Computer 1).
>
> * * * *
>
> The SOI looked at the profile of the computer (Target Media) and noticed it was running a Linux Operating System, as well as using LUKS. The SOI also noticed a VeraCrypt volume mounted on the Target Media named "VeraCrypt 1".
>
> * * * *
>
> The SOI also observed the presence of a TOR (The Onion Router) browser on the Target Media. The SOI also observed other folders labeled'oVeraCrypt2" and "VeraCrypt 3 also on the Target Media.
>
> * * * *
>
> The SOI looked at the contents of the VeraCrypt 1 volume and viewed some of the image files within this volume. The SOI saw approximately five or six images, maybe seven, of what the SOI identified as child pornography. The SOI then stopped looking at image files. The SOI indicated there were many additional images in the VeraCrypt 1 volume.
>
> The SOI also observed the Thunderbird email client installed on the Target Media. The SOI recalled there were many email messages within this client. The SOI also recalled a folder named ooto jenny," or something to that effect. The SOI looked in this folder and observed that it was also fuIl of what the SOI believed was child pornography.
>
> * * * *

> The SOI located an image of a Vermont Enhanced Driver's License, which was saved on the Target Media. The SOI provided this license in its email to the VSP.
> The SOI looked through the Target Media on or about June 16, 2021 at approximately 8:00 PM Eastern Time.

Doc. 5-3.

The application recounts another interview with the SOI on June 30, 2022.

The application relates that:

> The security vulnerability that he and his colleagues are researching (see paragraph 9(a), supra) identified a computer with an IP address that resolved to Germany. The user of this computer was "Scott."
>
> * * * *
>
> b. Based on the internal network configuration/information of Computer 1, the SOI suspected that Computer 1 was not at the same location as the IP address in Germany.
> c. The SOI was able to identify another computer (Computer 2) on the same local network as Computer 1. The SOI asked Computer 2 to report its public IP address. Computer 2 provided IP address, 209.99.193.74, which resolves to an ISP in Vermont.
> 1. The SOI provided the following analogy to explain the concept of what it did to identify the IP address for Computer 2: A computer on a home network using a Virtual Private Network (VPN) can make itself appear to be elsewhere. A second device on that same network, if not also using a VPN, is most likely, if accessed and queried as to the IP address it is using, to return an accurate public IP address. It will thus provide the actual physical location of the device.
> d. Based on the SOI's experience as a security researcher, and the below facts, the SOI believes that IP address 209.99.193.74 is the accurate location for the Target Media:
> 1. The user of Computer 1 was “Scott.”
> 2. Another computer in the same internal network as Computer 1 provided its IP address as 209.99.193.74.
> 3. The SOI located an image of a Vermont Enhanced Driver's License, issued to Scott I. Remick, of Bristol, Vermont, saved on the Target Media.

Doc. 5-3 at 10-11. The application then recounts the fact that the authorities determined the IP address was registered with Waitsfield and Champlain Valley Telecom and that the IP address had been used by Mr. Remick during the applicable time period. Doc. 5-3 at 11-12. Investigators determined that Mr. Remick and another individual, Gina Wrest, both lived at the Hardscrabble Road address. The application explains further that the authorities searched the internet and determined that Mr. Remick worked at Middlebury College as a Senior Technology Specialist, had his own computer repair business, and used the same phone number as Waitsfield and Champlain Valley Telecom provided. Doc. 5-3 at 12.

Authorities surveilled the Hardscrabble Road home on June 22, 2021, and determined that vehicles registered to Mr. Remick and Ms. Wrest were parked there. On the same day, the application recites, authorities were contacted by the Vermont Attorney General's office about a report from the National Center for Missing and Exploited Children (NCMEC). This was a report made by the SOI about the same incident in which the SOI hacked a computer alleged to belong to Mr. Remick. The NCMEC report contained the same information as the SOI provided to the VSP. Doc. 5-3 at 13-14. The report also reflects several specific claims that the SOI made: (1) that the computer owner was chatting with another person (possibly a minor) with whom the computer owner may have a sexual relationship; (2) that the computer owner "is communicating with Jeanie. It is believed that she may be a teenager. The reported person and Jeanie are either

trading images or having a relationship."; and (3) that the computer owner "will attempt to delete the images upon the arrival of law enforcement." Doc. 5-3 at 14. The NCMEC report provided an email address for the individual identified as "Jeanie."

The application next recounts a June 23, 2021, interview with the SOI in which the SOI described the images it saw on the computer.

> [T]he SOI provided a description of several of the child pornography and child exploitation images from memory; the SOI did not save any of the image files it viewed. A description of some of the files are below. The SOI did not recall the filenames for these image files, so I am referencing them as first, second, third, for purposes of this affidavit:
> a. First Image: A female child, approximately 10-14 years old, in a "69" position with a much older adult male. The male and this child were involved in a sex act together.
>
> * * * *
>
> b. Second Image: A female child, approximately 12-13 years old, fully nude with her legs spread wide open. No pubic hair or breast development was observed.
> c. Third Image: A possibly European teen, maybe Scandinavian, approximately 15-16 years old, topless with her breasts exposed.

Doc. 5-3 at 15.

Importantly, the SOI also revealed that it had installed two backdoors to the computer so that law enforcement could access the computer:

> [T]he SOI also advised it had installed two separate methods to access the Target Media at a later time, to which it referred as a "backdoor." The SOI installed the backdoors so law enforcement could access the Target Media remotely and without the user of the Target Media's knowledge in case the vulnerability that allowed it to access the Target Media no longer existed. The SOI also included a protocol in the backdoor whereby it regularly communicated from the Target Media to the SOI's computer (the Ping). The Ping was established to keep the

> backdoor open and viable. The Ping does not access content from, or communicate with, the Target Media; its sole function is to keep the communication line to the backdoor open.

Doc. 5-3 at 15-16.

After boilerplate language about the "characteristics of child pornographers," the application briefly addressed "the remote search technique" that was the major request for the remote access warrant. The application explains that the investigators believed that remotely accessing the computer was necessary and requested approval to use "the remote search technique." Doc. 5-3 at 17. However, the application did not explain the technique that would be used. Instead it offered that:

> The remote search of the Target Media will entail law enforcement remotely communicating with the Target Media in order to conduct an exfiltration of the information outlined in Attachment B to a government-controlled infrastructure, meaning government-controlled storage media. Law enforcement will not make any changes to the Target Media beyond any changes to metadata that will occur as a result of accessing data during the search.

Doc. 5-3 at 17-18.

Argument: The evidence obtained as a result of the remote-entry & Hardscrabble Road warrants must be suppressed for violations of the Fourth and Fifth Amendments.

The Fourth Amendment protects against unreasonable searches and seizures through its requirement that "no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The Second Circuit has noted that:

> [I]t is generally understood that "probable cause to search is demonstrated where the totality of circumstances indicates a 'fair probability that contraband or evidence of a crime will be found in a particular place.'" This required nexus between the items sought and the "particular place" to be searched protects against the issuance of general warrants, instruments reviled by the Founders who recalled their use by Crown officials "to search where they pleased."

United States v. Clark, 638 F.3d 89, 94 (2d Cir. 2011) (internal citations omitted). Ultimately, a judge issuing a search warrant must "make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238 (1983). A court reviewing a probable cause determination, generally gives "great deference" to the issuing judicial officers' determination that probable cause existed and will "simply" ensure that the judicial officer "had a substantial basis for concluding that probable cause existed." *United States v. Falso*, 544 F.3d 110, 117 (2d Cir. 2008) (quoting *Gates*, 462 U.S. at 236). Regardless, a reviewing court "may properly conclude that a warrant was invalid because the [judicial officer's] probable-cause determination reflected an improper analysis of the totality of the circumstances." *Id.* (internal citations omitted).

Courts recognize that searches of modern computer devices are highly invasive and "would typically expose to the government far more than the most exhaustive search of a house." *Riley v. California*, 573 U.S. 373, 396 (2014). The warrants in this case sought remote access to Mr. Remick's computers and home based on a fabulous tale told by an admitted hacker. The government took the fabulous tale on

faith and did little to confirm the most important parts of what the SOI told them. The investigation the government did conduct benefitted from the SOI's continued covert monitoring of the devices, monitoring that constituted a search, that was unapproved by the Court, and that was withheld from the Court. The warrant failed to establish probable cause to believe that child pornography would be found on the devices and must be suppressed. The warrant to search Mr. Remick's home was substantially identical and featured the same deficiencies. Because later warrants that led to the charges set forth in the superseding indictment were triggered only by the initial searches, that evidence must be suppressed as fruit of the poisonous tree.

I. The government violated the Fourth Amendment by utilizing a government agent, the SOI, to monitor the target computers without a warrant.

Discovery makes it clear that the SOI installed at least two backdoors to monitor the target computers and report back to the government. The SOI then relayed this information to agents, who utilized the information in planning and executing the investigation and searches. The government never obtained a warrant for this monitoring and withheld the details of the monitoring from this Court when it sought permission to remotely access the computers and to search Mr. Remick's home.

A. The SOI was a government agent.

The SOI was clearly a government agent in the lead up to the issuance and execution of the remote-entry and Hardscrabble Road warrants. The Second Circuit has explained that "[w]hen the government compels a private party to assist it in

conducting a search or seizure, the private party becomes an agent of the government, and the Fourth Amendment's warrant clause applies in full force to the private party's actions." *Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 829 F.3d 197, 214 (2d Cir. 2016) (*citing, inter alia, Coolidge v. New Hampshire*, 403 U.S. 443, 487 (1971)). Here, the SOI signed cooperation and immunity agreements that obliged it to assist the government in its investigation. The SOI then obtained information from the backdoors that it installed and the government utilized this information in the planning and execution of its investigation and searches.

B. The SOI's backdoors

While the remote-access and Hardscrabble Road warrant applications relate that the SOI installed a backdoor, it did not fully describe what the SOI did and how its backdoors functioned. Nor did the government have approval for the SOI's continued monitoring of the target computers. This monitoring was a search and violated the Fourth Amendment.

Specifically, the warrant application does not disclose that the backdoors installed by the SOI includes a monitoring function that informed the SOI when a "drive" has been "mounted," i.e., connected to the computer. Nor does it disclose that the backdoor informs the SOI when the target computer is restarted. It is clear that the government's strategy benefitted from this information because on June 23, 2021, discovery indicated the SOI suggested waiting until the targeted drive is mounted to "go in," which is exactly what happened. The government never had approval for this continued monitoring, which was a search and violated the Fourth

Amendment. The evidence seized as a result of this warrantless search should be suppressed as fruit of an illegal search.

II. The remote-access and Hardscrabble Road warrant applications fail to establish probable cause.

A. The warrant applications fails to establish that the SOI actually viewed child pornography; that is, images depicting minors engaged in sex acts or lasciviously depicting a minor's genitalia.

The warrant application fails to provide detail from which a judge could determine that the target computer actually possessed child pornography. While the warrant application reflects the SOI's *claim* that the computer owner possessed child pornography, the only images actually described in the application fail to provide detail (including the file names) from which a judge could determine that the SOI actually viewed child pornography on the target computers; i.e., images that depicted a minor engaged in a sex act or that depicted the lascivious exhibition of the minor's genitals. *See* 18 U.S.C. § 2256(2)(A).

Thus, the application fails to provide sufficient detail for a court to independently determine that the target computer likely contained images depicting minors. More specifically, the applications fail to explain how the SOI determined that the images involved a minor, how law enforcement determined that the SOI's recollections (as a whole or individually) were accurate, or how the SOI's appraisal of the subjects' ages were accurate. Rather, the applications state in a conclusory fashion that the first image involved "[a] female child, approximately 10-14 years old"; the second image involved "[a] female child, approximately 12-13 years old"; and the third image involved "[a] possibly European

teen, maybe Scandinavian, approximately 15-16 years old." Doc. 5-3 at 15. This is insufficient.

While the description of the first image does at least assert that a sex act was depicted, it fails to explain how the SOI and investigators determined the female was a minor. First, the description does not state that the female appeared to be prepubescent. Nor does the description cite the absence of physiological markers such as breast development or pubic hair. Instead, the description states that image was of a child "approximately 10-14 years old." Yet the wide range given—from 10 years and 1 day to 14 years and 364 days—and the fact that this is an *approximate* range makes it clear that the SOI had no idea how old the individual was and instead thought that the image involved a minor because the female appeared generically "young"[2] to the SOI. This is not sufficient.

The second image does indicate that that the SOI did not observe breast development or pubic hair but includes little more. The description does not indicate that the minor was prepubescent or provide any other reason to conclude that the image was of a minor. In short, the description does not discount the

[2] The government knew or should have known this was a very likely possibility because the SOI repeatedly claimed that the individual it hacked was trading child pornography with someone named Jean or Jeannie who the SOI believed might be a minor. Doc. 5-3 at 14. The SOI even provided an email address for Jean or Jeannie. The SOI must have formed this opinion based on images of this Jean or Jeannie. However, while Mr. Remick had a long-term romantic relationship with Jean Lin, and while Jean Lin may appear younger than her chronological age to many, now-Dr. Lin in fact graduated from college more than a decade ago and is a practicing physician in Vermont. By the time it sought the warrant, the government knew or should have known that the SOI had mistakenly concluded that Jean Lin might be a minor, when she was in fact not. This is one of the crucial facts that the government withheld when it sought the warrants challenged here.

likelihood that the female was simply small breasted, had shaved her pubic hair, was extremely thin, or had light-colored hair. Again, the fact that the SOI could cite nothing more than a wide approximate age range means that the SOI again thought the image depicted a minor because the female looked "young."

Also problematic is the fact that the description of the second image provides no reason to conclude that the image involved the lascivious depiction of a minor's genitalia. While the description indicates that the female had "her legs spread wide open," there is no additional description to support the conclusion that this is child pornography. The description does not indicate that the individual and her genitals are the focal point of the image or provide any other description of the setting to support the SOI's opinion that this was an image of child pornography.

The third image provides even less reason to conclude that the image depicts child pornography both because it does not depict a lascivious exhibition of genitals or a sex act and because it does not depict a minor. The description of "[a] possibly European teen" of "approximately 15-16 years old" who is "topless with her breasts exposed" fails to provide any details from which one could conclude the image involves a lascivious exhibition of the genitals. Likewise, without any further description of the individual, it again fails to provide any reason for the conclusion that the image depicted a minor other than that the SOI must have thought the individual looked "young."

These three descriptions are problematic for other reasons as well. First, the SOI reported that it had observed at least seven images of child pornography. Doc.

5-3 at 6. The fact that only these three images are described strongly suggests that investigators determined that the other images the SOI saw were not child pornography and that the SOI's assessment was incorrect. Second, the SOI stated that the seven images it saw "shook me to my core." Yet, the images actually described are not in keeping with this claim. Instead, the disconnect raises the distinct possibility that the SOI may have viewed images that seemed "pornographic" to him or her, that appeared to involve young individuals, but that were not child pornography. Third, the application provides no basis for a court to assess the SOI's accuracy in estimating age. Rather, the fact that the SOI could only cite broad "approximate" age ranges indicates on its face that the SOI has no expertise whatsoever in estimating age.

The present case differs from others where the descriptions were determined to be sufficient to establish probable cause that the images depicted minors. In general, the image[3] or a detailed description of the image is required for a court to determine that the image qualifies as child pornography (i.e., a depiction of a minor engaged in a sexual act or a lascivious depiction of a minor's genitalia). The images in question were not provided and the investigators did not observe them. The

[3] The SOI's failure to provide the images is telling in this case and stands in contrast to other cases where individuals stumble over images of child pornography. *United States v. Bonczek*, 2008 WL 4615853 (S.D.N.Y. Oct. 16, 2008) (maintenance employee took photo of child pornography images displayed on computer). Afterall, the SOI provided authorities with other images and could certainly have provided the actual images that he or she claimed to have viewed or a photo or printout of those images. The claim that the SOI could not have provided authorities with an image because doing so would have been illegal also fails. 18 U.S.C. § 2252(c) contains an affirmative defense where a limited number of images are possessed, deleted, and reported to the authorities. The SOI's activities would have fallen within this safe harbor.

descriptions related by the SOI are palpably inadequate. By contrast is this Court's decision in *United States v. Barker*, 2012 WL 12543 (D. Vt. Jan. 3, 2012). In *Barker*, the Court determined that descriptions provided by a FBI Special Agent investigator were adequate. The warrant explained that the agent had worked for 13 years as a Special Agent, including "several years at the FBI's Innocent Images Program." *Id.* at *1. The agent's description of the images addressed both the depicted individual's age and whether the image showed the lascivious depiction of genitalia or a sex act. The Court concluded that

> Special Agent Emmons described sufficient qualifications and experience to assess the ages of the children depicted in the images. By describing the images as depicting "prepubescent or pubescent minors" engaging in sexually explicit or lewd and lascivious conduct, the affidavit excludes virtual child pornography, "which by definition does not depict minors[.]"

Id. at *6 (citation omitted).

This case is also different from the Ninth Circuit's decision upholding a state warrant with limited description of the images. *United States v. Battershell*, 457 F.3d 1048, 1049 (9th Cir. 2006). Although the description of the images was limited in *Battershell*, there were other factors that supported the probable cause determination. In *Battershell*, the authorities were alerted by two individuals who both "saw pictures of 'kids having sex,'" which was reflected in the warrant application. *Id.* at 1049. Moreover, when the police came to investigate, the application explained that two officers then viewed several images, including one which "showed 'a young female (8–10 YOA) naked in a bathtub. The second picture

showed another young female having sexual intercourse with an adult male. This confirmed that the pictures were illegal to obtain.'" *Id.* The Ninth Circuit determined that the warrant application's recitation that four individuals who saw images of young children engaged in sex acts supported the probable cause determination that there was a reasonable probability that contraband would be found on the computer. *Id.* at 1053. This stands in stark contrast with the case at hand where no one other than the SOI observed the images and the SOI could provide only very approximate ages and the most generalized description of the images.

B. The warrant and warrant application fail to particularly identify the place to be searched because it contains no information that narrows the search to the device identified by the SOI or that specifically identifies the device identified by the SOI.

The Fourth Amendment's particularity requirement, which outlaws sweeping, general warrants, has two components: it requires a sufficiently clear description of both (1) "the place to be searched, and (2) the persons or things to be seized." U.S. Const. amend. IV. While the SOI hacked into a particular computer and allegedly saw child pornography on that computer, that computer was not identified by the hacker or the government in its warrant application (such as by the Global Unique Identifier that such devices have or otherwise). Without such an identification, the warrant application was overbroad and sought access to all the devices connecting through a particular Waitsfield and Champlain Valley Telecom account (it sought "Electronically stored information on digital devices and media accessing the

Internet through Waitsfield and Champlain Valley Telecom account 200155513."). Doc. 5.

The lack of particularity is particularly evident given the fact that the SOI explained clearly that he or she had hacked into a particular device. The breadth of the government's request is striking also because the SOI and the authorities knew that more than one device utilized the network. The SOI explained that while the target computer had cloaked its IP address, another computer on the network was not cloaked and readily identified what the SOI believed to be the true IP address. Doc. 5-3 at 10. Functionally, this was the same as seeking a warrant to search the entirety of a building that is in fact comprised of separate apartment units. *United States v. Bermudez*, 526 F.2d 89, 96–97 (2d Cir. 1975) ("Since the warrant could have permitted a search of the entire building, and there was probable cause for search of the bottom floors only, the warrant was defective due to overbreadth and the materials seized were properly suppressed."). It has long been the case that this sort of warrant is overbroad and will be struck down on particularity grounds. *See United States v. Bershchansky*, 788 F.3d 102, 111 (2d Cir. 2015) (affirming grant of motion to suppress where magistrate judge issued warrant to search for child pornography in apartment 2 and agents searched apartment 1). The Court should apply this rule here and suppress any evidence seized as a result of the remote-entry warrant.

C. The warrant application contains no information from which a judge could determine how the remote access would occur or whether a tested and reliable method would be used in violation of the Fourth Amendment and the Fifth Amendment's Due Process Clause.

The remote-access warrant's prime request was that the court permit the government to access the target remotely in order to seize evidence. Incredibly, however, the application presents only a circular claim that the computers would be remotely accessed by remotely accessing them.

> The remote search of the Target Media will entail law enforcement remotely communicating with the Target Media in order to conduct an exfiltration of the information outlined in Attachment B to a government-controlled infrastructure, meaning government-controlled storage media. Law enforcement will not make any changes to the Target Media beyond any changes to metadata that will occur as a result of accessing data during the search.

Doc. 5-3 at 17-18. In sum, the remote-access warrant application offered only a circular claim that the computers would be remotely accessed by remotely accessing them.

Just as the decision to utilize other extraordinary methods to effectuate a search is subject to judicial review, the use of the unknown and untested methods to gain access to these computers, to search them, and to then collect evidence is unreasonable and violates the Fourth Amendment. Like other Fourth Amendments inquiries, "the manner in which a warrant is executed is subject to later judicial review as to its reasonableness." *Dalia v. United States*, 441 U.S. 238, 258 (1979). "The general touchstone of reasonableness which governs Fourth Amendment analysis ... governs the method of execution of the warrant." *United*

States v. Ramirez, 523 U.S. 65, 71 (1998) (internal citation omitted). Here, the government relied entirely on the SOI and utilized the SOI's untested and unverifiable hacking method to gain access to the target computers. This violated the Fourth and Fifth Amendments and any evidence recovered must be suppressed.

III. The Court should suppress any evidence recovered from the search of the Dell computer because the affidavits supporting it contained materially false or misleading statements or omissions. The Court should hold a *Franks* hearing.

A warrant is susceptible to a challenge, where the supporting affidavit contains deliberately or recklessly false statements or misinformation, or where deliberate or reckless omissions have been made. *United States v. Canfield*, 212 F.3d 713, 717-718 (2d Cir. 2000) (citing *Franks v. Delaware*, 438 U.S. 154, 164- 172 (1978)). Where necessary information has been omitted or false information included, the seized evidence will be suppressed if "'(1) the claimed inaccuracies or omissions are the result of the affiant's deliberate falsehood or reckless disregard for the truth; and (2) the alleged falsehoods or omissions were necessary to the [issuing] judge's probable cause finding.'" *Id.* at 717-718 (quoting *United States v. Salameh*, 152 F.3d 88, 113 (2d Cir. 1998)); *see also United States v. Rajaratnam*, 719 F.3d 139, 146 (2d Cir. 2013) (observing that under *Franks*, a defendant must show that there were misrepresentations or omissions in the search warrant affidavit that were (1) intentional or reckless, and (2) material to the probable cause determination). A warrant that violates *Franks* is not subject to the good-faith exception to the exclusionary rule announced in *Leon*. *United States v. Leon*, 468 U.S. 897, 923

(1984). The Court should suppress any evidence obtained as a result of the remote-entry and Hardscrabble Road searches.

The warrant applications contains material omissions as well as statements that the government knew or should have known were false. To begin with, the warrant application fails to inform the magistrate that the remote access will be achieved through unknown, untested, and unverified methods. As noted above, the application explains the remote entry that is contemplated through the circular observation that the remote entry will be achieved by remotely entering the devices. Doc. 5-3 at 17-18. In fact, on July 1st and 2nd as the authorities were applying for the warrant, agents were still developing the programs by which the devices would be accessed. Further, these were not "stock" law enforcement programs that had been previously used and validated. Instead, agents simply took the SOI's hacking tools and utilized those to recreate the hack of the target computers. This was not disclosed to the reviewing judge. These were material facts and had the government disclosed that the remote access would be accomplished using an unknown, untested, and unverified method provided by the hacker that originally broke into the computer system, the magistrate judge would have declined to issue the warrant.

The application omits other facts the government knew or should have known about the SOI's hacking. For example, while the application indicates that the backdoors installed by the SOI had limited functionality, in fact this was not true. As noted above, it was actually the case that the backdoors installed by the SOI had

a monitoring function that informed the SOI when the suspected "drive" has been "mounted," i.e., connected to the computer. Nor does the warrant application disclose that the backdoor informs the SOI when the target computer is restarted. It is clear that the government's strategy benefitted from this information because on June 23, 2021, discovery indicates the SOI suggested waiting until the drive is mounted to "go in," which is exactly what happened when the government executed the remote-entry warrant. This was a material omission because had the government fully described the SOI's backdoors, the magistrate judge would have understood that the government's agent was already monitoring the devices and engaging in an unlawful search in violation of the Fourth Amendment.

Given the fabulous claim made by the SOI, one might conclude that the government should have further investigated before seeking a warrant. In fact, investigators had information from other sources that detracted from the probable cause claim and withheld that information from the Court. For example, the government received NCMEC's report about the SOI's Cybertip. While the government cites the fact of the SOI's Cybertip as something that weighs in favor of probable cause, it conveniently omits any substantive discussion of the NCMEC report, which weighs strongly against the SOI's claims.

NCMEC maintains a large repository of child pornography as well as a large investigative database of prior reports and investigations. The report received by the Vermont investigators included the results of NCMEC's queries of its databases. These queries all turned out negative. In short, when NCMEC searched for the IP

addresses as well as the names, addresses (both physical and electronic), and phone numbers provided by the SOI it got no hits. The government withheld this information. Moreover, while it featured the fact that authorities determined that the SOI has no criminal history, it fails to inform the reviewing judge that Mr. Remick also has no criminal history, a fact the government was aware of.

The government did other work as well. One of the SOI's prominent claims was that the individual it hacked was trading child pornography with someone named Jean or Jeannie who the SOI believed might be a minor. Doc. 5-3 at 14. The SOI even provided an email address for Jean or Jeannie. The SOI must have formed this opinion based on images of this individual that it found when it hacked the computers. However, while Mr. Remick had a long-term, romantic relationship with Jean Lin, and while Jean Lin may appear younger than her chronological age to some individuals, now-Dr. Lin in fact graduated from college more than a decade ago and is a practicing physician in Vermont. By the time it sought the warrant, the government knew that the SOI had mistakenly concluded that Jean Lin might be a minor, when she was in fact not. Yet, this fact was not included. This is an especially crucial fact because as explained above, the application has little information detailing how or why the SOI concluded that the individuals depicted in the images it saw were minors. The fact that the SOI mistakenly concluded that Jean or Jeannie was a minor would significantly undercut any claim that the SOI correctly interpreted the age of the individuals it saw in the images it thought were child pornography.

IV. The good-faith exception will not save the searches because the purpose of the exclusionary rule will be served, because the warrants palpably lacked probable cause, and because the warrants contained material omissions and falsities.

It is axiomatic at this point that "suppression is not an automatic consequence of a Fourth Amendment violation." *Herring v. United* States, 555 U.S. 135, 137 (2009). "Instead, the question turns on the culpability of the police and the potential of exclusion to deter wrongful police conduct." *Id.* There are also circumstances in which the good faith exception will not apply:

> [T]here are four circumstances in which the good-faith exception does not apply: "(1) where the issuing [judge] has been knowingly misled; (2) where the issuing [judge] wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient [such as by failing to particularize the place to be searched or the things to be seized] that reliance upon it is unreasonable."

Falso, 544 F.3d at 125. Here, the good faith exception will not apply because the purpose of the exclusionary rule will be served, because the warrant was objectively lacking in indicia of probable cause, and because the government intentionally or recklessly withheld material information from the issuing magistrate in reckless disregard of Mr. Remick's Fourth Amendment rights.

To begin with, the good faith exception should not apply here because the purpose of the exclusionary rule will be served. The good faith exception is based on the premise that the purpose of the exclusionary rule—deterring "deliberate, reckless, or grossly negligent conduct," *Herring*, 555 U.S. at 144—will not be served when the error is the magistrate's and not the agents. Thus, "[p]enalizing the officer

for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." *United States v. Leon*, 468 U.S. 897, 921 (1984). Here, the case was investigated by, and then the warrant was drafted and executed by the same agent, Agent McCullagh. This, then, is one of those cases where penalizing the agents for their own error *will* "logically contribute to the deterrence of Fourth Amendment violations." *Id.* As explained below, this also is one of those cases where the government acted in "'deliberate,' 'reckless,' or 'grossly negligent' disregard for Fourth Amendment rights [and] the deterrent value of exclusion is strong and tends to outweigh the resulting costs." *Davis v. United States*, 564 U.S. 229, 238 (2011).

Next, the warrant application lacked any objective indication of probable cause, for all the reasons stated above. The warrant application failed to identify the computer(s) it sought to search or differentiate that computer from other computers on the network. The application relied on the SOI who was not able to provide copies of the images it thought were child pornography or describe them in enough detail for a magistrate to conclude they depicted child pornography. Nor did the warrant application identify the devices it sought access to with the particularity required by the Fourth Amendment. The warrant also failed to identify the remote entry method in any detail.

Even more troublesome is the information withheld by the warrant application. When this information, including the fact that one individual the SOI

thought was a minor was well over age 18, is taken into account, there is no question that the warrant could not have been issued.

Finally, the government's willingness to credit and rely on the SOI's fabulous tale was the kind of recklessness that shows a "heedless indifference to the subject's Fourth Amendment rights" and the good faith exception should therefore not apply. *United States v. Raymonda*, 780 F.3d 105, 123 (2d Cir. 2015) (Chin, J., dissenting); *United States v. Rajaratnam*, 719 F.3d 139, 154 (2d Cir. 2013) ("the 'reckless disregard' aspect of a *Franks* inquiry can sometimes be inferred from the omission of critical information in a wiretap application."); *Rivera v. United States*, 928 F.2d 592 (2d Cir. 1991) ("recklessness may be inferred where the omitted information was 'clearly critical' to the probable cause determination") For all these reasons, the Court should conclude that the good faith exception does not apply.

V. Later warrants relied on the earlier searches in at least two ways and must be suppressed as fruit of the poisonous tree.

The later warrants sought by the government must be suppressed as fruit of the poisonous tree. These warrants were in no way independent of the earlier warrants and investigation for at least two reasons. First, these later warrants all indicate that it was the earlier searches and arrests that led to the later investigation into Mr. Remick's relationship with M.C. and other individuals. For example, these warrants all note that "Remick's arrest on July 7, 2021, drew interest from the media. Since Remick's arrest, several people have come forward to provide me with information about Remick. Specifically, these individuals

alleged that Remick engaged in sexual activity with them when they were minors." *See, e.g.,* Doc. 34-3 at 16.

The later warrants rely on the earlier warrants in a second way. Each of the later warrants attaches the earlier warrant(s) as support for the issuance of the later warrants. In short, but for the government's earlier investigations and searches that Mr. Remick has challenged, the government would never have received the information that led it to seek the later warrants. The later evidence is thus fruit of the poisonous tree and must be suppressed.

CONCLUSION

For the reasons stated above, Mr. Remick respectfully requests that the Court suppress all evidence obtained as a result of the remote-access and Hardscrabble Road warrants. All evidence obtained as a result of the warrants issued later should also be suppressed as fruit of the poisonous tree.

Dated: December 5, 2022

MICHAEL L. DESAUTELS
Federal Public Defender

By: */s/ Steven L. Barth*__
Steven L. Barth
Assistant Federal Public Defender

Office of the Federal Public Defender
District of Vermont
95 Pine Street, Suite 150
Burlington, Vermont 05401
(802) 862-6990
Counsel for Scott Remick